Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

813

Vragen van de leden **Oosenbrug** en **Kerstens** (beiden PvdA) aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Staatssecretaris van Sociale Zaken en Werkgelegenheid over *het bericht dat jaaropgaven van 1.712 cliënten van enkele Groningse sociale diensten per ongeluk aan een andere cliënt zijn toegestuurd* (ingezonden 23 november 2016).

Antwoord van Minister **Plasterk** (Binnenlandse Zaken en Koninkrijksrelaties) mede namens de Staatssecretaris van Sociale Zaken en Werkgelegenheid (ontvangen 20 december 2016)

Vraag 1
Kent u het bericht dat jaaropgaven van 1.712 cliënten van enkele Groningse sociale diensten per ongeluk aan een andere cliënt zijn toegestuurd?[1]

Antwoord 1
Ja.

Vraag 2
Hoe beoordeelt u de situatie waarin de jaaropgaven van 1.712 cliënten van Groningse sociale diensten aan een cliënt verzonden zijn terwijl er op deze jaaropgaven gegevens terug te vinden zijn waarmee identiteitsfraude gepleegd zou kunnen worden?

Antwoord 2
Ik hecht er aan te benadrukken dat wat er is voorgevallen buitengewoon ongelukkig is voor alle betrokkenen en dat betreur ik. Een kwaadwillende zou misbruik kunnen maken van gegevens. Het risico is klein, maar misbruik van persoonsgegevens valt niet uit te sluiten.

Vraag 3
Deelt u de mening dat het incident een datalek betreft? Doet de Autoriteit Persoonsgegevens onderzoek naar het genoemde datalek? Zo ja, wat is de stand van zaken van dat onderzoek? Zo nee, waarom niet?

---

[1] http://nos.nl/artikel/2143831-vrouw-ontvangt-jaaropgaven-van-ruim-1700-andere-klanten-sociale-dienst.html

ah-tk-20162017-813
ISSN 0921 - 7398
’s-Gravenhage 2016

Antwoord 3
Volgens de definitie die de Autoriteit Persoonsgegeven hanteert is er sprake van een datalek als zich een beveiligingsincident heeft voorgedaan waarbij persoonsgegevens verloren zijn gegaan of onrechtmatige verwerking van persoonsgegevens redelijkerwijs niet kan worden uitgesloten. De vier gemeenten waar Werkplein Ability voor werkt, de gemeenten Bedum, De Marne, Winsum en Eemsmond, hebben naar eigen zeggen het incident gemeld bij de Autoriteit Persoonsgegevens (AP) en zijn daarmee van mening dat het in dit incident om een datalek gaat. De Autoriteit Persoonsgegevens doet geen mededelingen over eventuele onderzoeken.

Vraag 4
Heeft u er zicht op hoe vaak datalekken bij gemeenten en bij organisaties binnen het sociaal domein plaatsvinden en wat de voornaamste oorzaken van deze datalekken zijn? Zo nee, waarom niet en bent u bereid hier onderzoek naar te doen?

Antwoord 4
Vanaf 1 januari 2016 zijn ook gemeenten verplicht om datalekken te melden bij de AP. Ik heb dan ook niet de beschikking over de exacte cijfers van de AP over datalekken in het sociale domein. In een interview van 7 oktober jongstleden met NU.nl verklaart de voorzitter van de AP Aleid Wolfsen dat er sinds de invoering van de meldplicht datalekken op 1 januari 2016, tot de datum van het interview bijna 4.000 meldingen zijn geregistreerd bij de AP[2]. Ongeveer 10% van die meldingen is afkomstig van een gemeente. Jaarlijks rapporteert de AP in het jaarverslag, maar de AP doet geen mededelingen over eventuele (lopende) onderzoeken.

Vraag 5
Herinnert u zich uw antwoorden op de vele eerdere vragen die gesteld zijn over de beveiliging en verwerking van persoonsgegevens in gemeenten?[3]

Antwoord 5
Ja.

Vraag 6
Deelt u de mening dat datalekken nog te vaak voorkomen bij gemeenten? Zo ja, op welke manier gaat u gemeenten verder stimuleren om adequate maatregelen te nemen om datalekken zoveel als mogelijk te voorkomen en om aan de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) te voldoen? Op welke wijze worden ook organisaties binnen het sociaal domein hierbij betrokken?

Antwoord 6
Vanzelfsprekend is elke datalek er één te veel, zeker als het persoonsgegevens betreft en is zorgvuldigheid geboden. Het is een goede zaak dat gemeenten melden aan de AP. De gemeenten hebben de BIG als normenkader voor informatiebeveiliging waarbij gestructureerd wordt aangegeven wat de doelstellingen van de technische, organisatorische en fysieke beveiligingsmaatregelen zijn. Implementatie verschilt per situatie en is een continu proces van plannen, uitvoeren, controleren en bijstellen. Elke gemeente blijft afzonderlijk verantwoordelijk voor de eigen informatiebeveiliging. De VNG heeft er bij gemeenten op aangedrongen extra aandacht te besteden aan informatiebeveiliging in samenwerkingsverbanden, vooral waar het een samenwerking met ketenpartners betreft. De VNG biedt hiervoor praktische handreikingen zoals de handreiking informatieveiligheid en intergemeentelijke samenwerkingsverbanden. Daarbij biedt de Informatie Beveiligingsdienst (IBD) van de VNG/KING verdere ondersteuning door middel van preventie en preventieadvies, incidentcoördinatie en kennisdeling.

---

[2] http://www.nu.nl/internet/4332988/privacywaakhond-start-tientallen-onderzoeken-meldingen-datalekken.html«
[3] Tweede Kamer, vergaderjaar 2015–2016, Aanhangselnummers 1613, 2076, 2401, 2643 en 2943.

Vraag 7
Bent u van mening dat de informatiesystemen van gemeenten en organisaties binnen het sociaal domein voldoende beveiligd zijn tegen datalekken? Is het bij al deze systemen mogelijk de veiligheid en gebruiksvriendelijkheid te verbeteren om zo datalekken in de toekomst te voorkomen? Zo ja, bent u voornemens samen met gemeenten te bekijken waar aanpassing en/of opwaardering van de huidige informatiesystemen nodig is? Zo nee, ziet u mogelijkheden om samen met gemeenten te onderzoeken waar de kwetsbaarheden in de systemen zitten en zo te komen tot een doelgerichtere aanbesteding van deze software in de toekomst?

Antwoord 7
Alle organisaties zijn zelf verantwoordelijk voor het beveiligen van de door hen gebruikte informatiesystemen. Het gaat juist om de combinatie van mens en systeem. Uit mijn contact met de IBD blijkt dat een groot deel van datalekken bij gemeenten voortkomen uit menselijke fouten. De IBD wijst gemeenten op maatregelen die hiertegen kunnen worden genomen. Ook werken gemeenten en samenwerkingsverbanden samen met VNG en KING aan het verbeteren van de veiligheid, gebruiksvriendelijkheid en interoperabiliteit van hun ICT-systemen. Behalve de BIG helpt het Gemeentelijk Model Architectuur (GEMMA), de landelijke referentiearchitectuur voor gemeenten. GEMMA helpt gemeenten en ketenpartners om (ICT-)ontwikkelingen in samenhang aan te sturen en aan te sluiten op landelijke voorzieningen. Ook zijn de Gemeentelijke Inkoopvoorwaarden Bij IT (GIBIT) ontwikkeld, die dit najaar van kracht zijn geworden en gemeenten en gemeentelijke samenwerkingsverbanden verder ondersteunen in het formuleren van passende en effectieve voorwaarden voor de levering, het gebruik en het onderhoud van IT-middelen, waaronder software en daarbij geldende (open) standaarden naar de verschillende leveranciers.

Vraag 8
Zijn de informatiesystemen van gemeenten en organisaties binnen het sociaal domein voldoende toegerust om te kunnen voldoen aan de eisen die worden gesteld vanuit de nieuwe privacyverordening die vanaf 2018 van kracht is? Zo nee, zal er dan een aanpassing plaatsvinden van de lopende contracten met de aanbieders van de software om gemeenten en organisaties binnen het sociaal domein aan te laten sluiten op de nieuwe privacywetgeving en richtlijn?

Antwoord 8
Gemeenten zijn, net als alle andere organisaties, ieder voor zich verantwoordelijk voor het toepassen van en voldoen aan de eisen van de komende Algemene Verordening Gegevensbescherming (AVG). Uitgangspunt is dat eenieder, gemeenten en de leveranciers, op het tijdstip dat de verordening van kracht wordt voldoet aan de gestelde normen. Waar nodig worden de komende tijd werkwijzen, afspraken en producten aangepast om aan de nieuwe regels te voldoen. Gemeenten hebben daar een aantal mogelijkheden voor, zoals privacy by design en impactanalyses en uitvoeringstoetsen. Met privacy by design kunnen organisaties daarnaast tijdens de ontwikkeling van producten en diensten zoals informatiesystemen al rekening houden met privacyverhogende maatregelen om verantwoorde en zorgvuldige omgang met persoonsgegevens technisch af te dwingen. Ook het uitvragen of laten uitvoeren van impactanalyses en uitvoeringstoetsen voor het gemeentelijk domein behoort tot de mogelijkheden. Gemeenten kunnen zich een beeld vormen over wat er op ze af gaat komen. Er hebben mij geen signalen bereikt dat gemeenten en de leveranciers niet aan de gestelde normen kunnen voldoen wanneer de verordening van kracht wordt.

Vraag 9
Is er voldoende kennis bij gemeenten en organisaties binnen het sociaal domein aanwezig om tijdig aan te kunnen sluiten op de nieuwe privacywetgeving en richtlijn? Zo nee, op welke wijze gaat u gemeenten ondersteunen om aan de nieuwe privacywetgeving en richtlijn te kunnen voldoen?

Antwoord 9
Toenemende digitalisering, ketensamenwerking en nieuwe regelgeving maken het noodzakelijk om continu te werken aan kennisopbouw op het gebied van bescherming van de privacy. Hierbij worden gemeenten onder andere ondersteund door VNG en KING. In samenspraak met de gemeenten heeft de VNG een position paper privacy opgesteld met actiepunten. Deze actiepunten worden door de VNG en KING uitgewerkt tot een beleids- en ondersteuningsprogramma. Ook de IBD speelt daarbij een rol met het ontwikkelen van operationele kennisproducten waaronder de leaflet over meldplicht. VNG en KING ondersteunen de gemeenten met de invoering van de AVG en de inrichting van de functie van Functionaris Gegevensbescherming die gemeenten, al dan niet in samenwerking met andere gemeenten, verplicht moeten aanstellen. Hiervoor worden gerichte (netwerk)bijeenkomsten georganiseerd en producten, waaronder handreikingen en opleidingen, ontwikkeld. Deze kennisopbouw wordt, waar relevant, specifiek gericht op verschillende beleidsdomeinen, waaronder het sociaal domein.